

Cyber

Pro

Latest
CYBERSECURITY
→ Articles

Best Cybersecurity Tools for
Companies in the USA

Top 5 Antivirus Software for
Businesses in 2025: An In-Depth
Review



**MATHIEU
GORGE**
CEO
VigiTrust

The Most
Revolutionary
Integrated Risk
Management
Company to Look
for in 2025

Redefining
Cybersecurity: How

VIGITRUST

is Pioneering a Safer
Digital Future



How about showcasing your products to
90,000+ C-suite Subscribers?

To get recent updates of our magazines

info@cybrpro.com



Address:

Cyber Pro, 1985, Henderson Rd,
Columbus, Ohio, 43220

Follow Us On:



For Editorial Concerns:

editor@cybrpro.com

For Sales & Branding Enquiries:

sales@cybrpro.com

For Subscription:

info@cybrpro.com

Creative Content Editor

Gabriel G.

PR & Marketing Coordinator

Ivy T.

Creative Design Head

Alice G.

Social Media Manager

Lisa W.

Marketing Coordinator

Olivia M.

Business Development Executive

Matthew S.

Digital Circulation Manager

Joseph B.



SUBSCRIBE US

PUBLISHER

Cyber Pro

This list is **NOT** a ranking. The companies on listed in magazine serve different aspects of the market, making ranking them in any order except revenue impossible and unfair.
We try to bring a perfect platform for business organization to showcase their valued products/ services.

Copyrights © Cyber Pro | 2024. All Rights Reserved. The images and content included in this magazine should not be copied, transferred or reproduced in any form or by any means, electronics, mechanical, photocopying, recording, otherwise, without proper permission from Cyber Pro. Cyber Pro solely owns all the reprint rights.



As we stand on the cusp of 2025, the digital landscape continues its relentless expansion, ushering in unprecedented opportunities alongside an equally unprecedented surge in cyber threats. The financial sector, in particular, finds itself at the epicenter of this duality.

This is precisely why the special issue of Cyber Pro Magazine, "The Most Revolutionary Integrated Risk Management Company to Look for in 2025," shines a well-deserved spotlight on organizations that are not merely reacting to threats but proactively shaping a safer digital future. And among the select few, one name stands out for its visionary approach and tangible impact: VigiTrust.

In a world where security silos often lead to vulnerabilities, VigiTrust has emerged as a beacon of integrated excellence. Their revolutionary SaaS platform, the VigiOne Integrated Risk Management System, is more than just a tool; it's a comprehensive ecosystem designed to empower organizations to fundamentally transform their approach to cybersecurity.

At the heart of VigiTrust's groundbreaking success and its distinctive vision is Mathieu Gorge, the company's CEO and an internationally recognized cybersecurity expert. Mathieu's journey into cybersecurity is as unconventional as it is inspiring. Unlike many industry leaders who emerged from traditional IT backgrounds, Mathieu's academic foundation in languages, marketing, and law has equipped him with a unique perspective, allowing him to unravel complex security challenges and articulate them in accessible terms. This multidisciplinary understanding underpins his philosophy that "Cybersecurity isn't just a technological challenge—it's a human one. It requires collaboration, education, and a proactive mindset to truly make an impact."

A handwritten signature in white ink that reads "Gabriel". The signature is stylized with a large, flowing 'G' and a long, sweeping underline that extends to the right.

08

COVER STORY

Redefining Cybersecurity:
How VigiTrust is Pioneering
a Safer Digital Future

18

ARTICLE

Best Cybersecurity
Tools for Companies in
the USA

28

ARTICLE

Top 5 Antivirus Software for
Businesses in 2025: An In-
Depth Review

STREET
COUN

Real photo of La Reforma prison, San José, Costa Rica.





Every month, more than
600 bank phone scams
are recorded from prisons.

 **credix**
WE DON'T CALL

Redefining Cybersecurity : How VigiTrust is Pioneering a Safer Digital Future

“As we speak, cybercrime is expected to cost the global economy a staggering \$10.5 trillion annually.”

Cyberattacks are becoming more sophisticated every day, and businesses are grappling with the reality of an increasingly dangerous digital industry. Breaches regularly make headlines, affecting everything from small to multinational corporations and leaving devastating financial, reputational, and operational consequences. However, the numbers only tell part of the story. Beneath the surface lies a global race against time as organizations attempt to outpace cybercriminals and ensure that critical data remains protected.

But how can we protect our future in a constantly connected world and under threat? The question looms large.

This is where **VigiTrust** comes into the picture—a company at the cutting edge of cybersecurity innovation. With its revolutionary SaaS platform, the VigiOne Integrated Risk Management System, and its trusted 5 Pillars of Security Framework™, VigiTrust is empowering organizations across the globe to transform their approach to cybersecurity.

At the heart of this transformation is **Mathieu Gorge**, CEO of VigiTrust and an internationally recognized cybersecurity expert. Known for his ability to simplify complex security challenges, Mathieu has spent nearly two decades helping businesses build sustainable cybersecurity strategies.

“Cybersecurity isn't just a technological challenge—it's a human one,” Mathieu emphasizes. “It requires collaboration, education, and a proactive mindset to truly make an impact.”

Under his leadership, VigiTrust has created innovative tools and enabled a thriving global ecosystem of cybersecurity, ensuring the company is at the forefront of protecting the digital economy. This feature explores how VigiTrust, under Mathieu's leadership, is revolutionizing cybersecurity and paving the way for a safer digital future for all.

A portrait of Mathieu Gorge, CEO of VigiTrust, in a dark blue suit and white shirt. He is standing outdoors with a blurred background of a boat. The image is framed by a red and white diagonal graphic element.

Cover *Story*

Mathieu Gorge
CEO | VigiTrust

A man with short dark hair, wearing a dark blue suit jacket over a white button-down shirt, stands outdoors. His hands are clasped in front of him. The background is a soft-focus view of trees with yellow and orange leaves, suggesting an autumn setting. A thick red curved line runs along the top and right edges of the page.

Cover *Story*

“

Cybersecurity isn't just a technological challenge—it's a human one. It requires collaboration, education, and a proactive mindset to truly make an impact.”

The Visionary behind VigiTrust

At the core of VigiTrust's story is Mathieu, a founder with a passion for problem-solving and a knack for thinking outside the box. Unlike traditional cybersecurity leaders, Mathieu's journey into the field began without formal IT training. Instead, his academic background in languages, marketing, and law, combined with his exposure to security-focused organizations early in his career, shaped his understanding of the complexities surrounding data protection and compliance.

With 25+ years of experience, Mathieu has become an expert in various security frameworks such as PCI DSS, GDPR, HIPAA, and ISO 27001. His active participation in global think tanks and security associations has allowed him to build a robust network of professionals dedicated to addressing cybersecurity challenges collaboratively. He has also served as the President of France Ireland Chamber of Commerce (2017-2019), President of CCEF (2022-2025) and now Vice President – Advising government (2025- present), and Board member FrenchTech Dublin since 2022.

5 Pillars of Security and Success

Since its inception, VigiTrust has achieved significant milestones that have shaped its identity as a leader in Integrated Risk Management. One of the company's most groundbreaking achievements is the development of the **VigiTrust 5 Pillars of Security Framework™**. This innovative framework provides organizations with a structured approach to managing risk and compliance across five critical areas:

1. **Physical Security:** Ensuring the safety of physical assets and facilities, including access control and environmental security.
2. **People Security:** Focusing on training and awareness to mitigate human-related risks, often the weakest link in cybersecurity.
3. **Data Security:** Protecting sensitive information through encryption, secure storage, and access controls.
4. **Infrastructure Security:** Safeguarding IT infrastructure, networks, and systems against cyber threats.
5. **Crisis Management:** Preparing for and responding to cybersecurity incidents to minimize damage and ensure business continuity.

The creation of the **VigiTrust Global Advisory Board** marked another defining moment. This non-commercial think tank brings together industry experts, regulators, and law enforcement professionals to foster collaboration and knowledge-sharing. By leveraging the collective expertise of its members, VigiTrust stays ahead of emerging trends, ensuring that its solutions address the real-world challenges businesses face.

Innovative Cybersecurity Solutions

VigiTrust's portfolio of solutions is designed to address the diverse needs of modern organizations. These include:

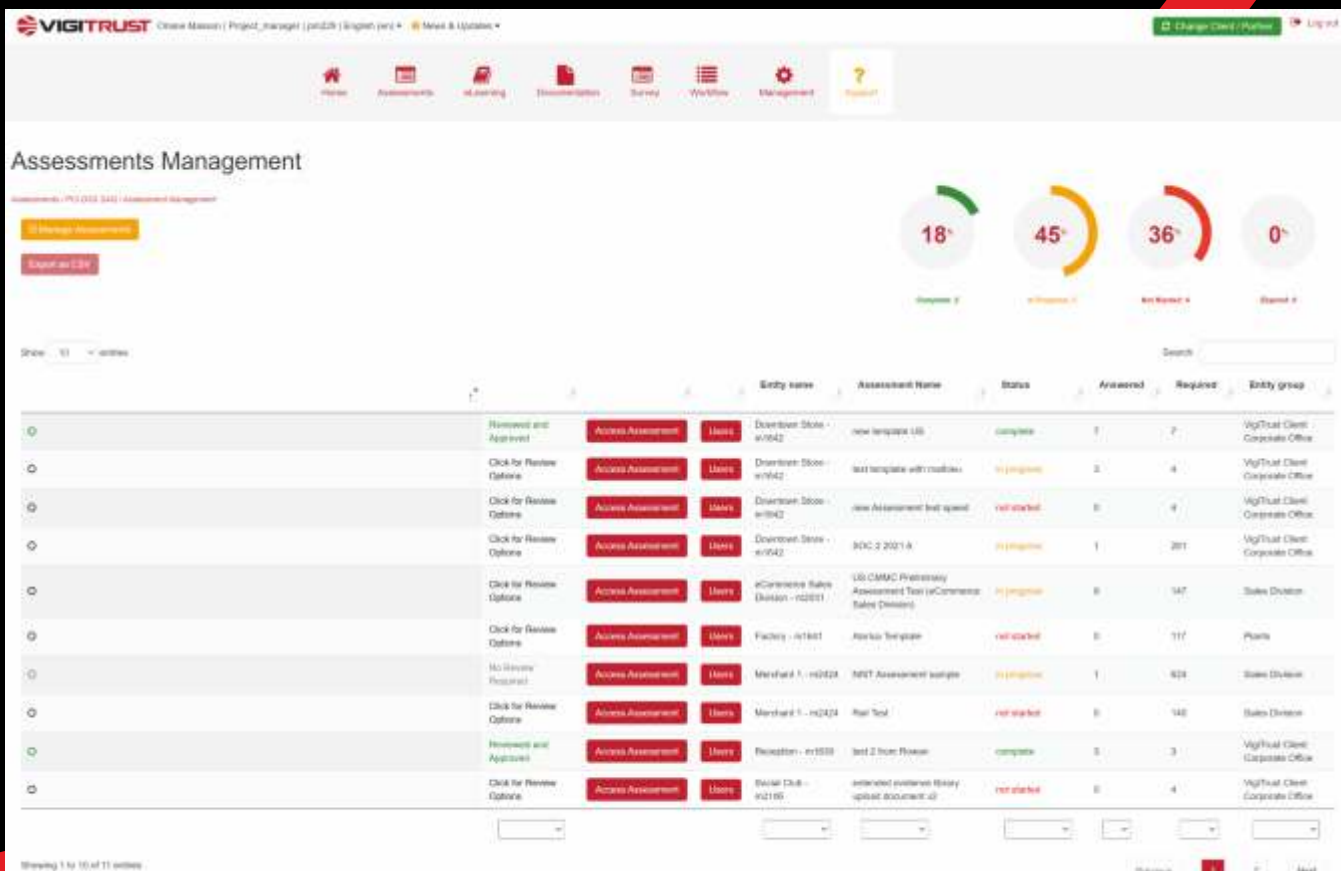
VigiOne Platform: The flagship offering of VigiTrust, the VigiOne platform provides a unified solution for managing cybersecurity, compliance, and risk. It enables organizations to assess their security posture, identify vulnerabilities, and implement corrective actions in real time.

Compliance Management: VigiTrust specializes in helping organizations navigate complex regulatory environments. Whether it's GDPR, PCI DSS, HIPAA, or CCPA, VigiTrust's solutions ensure that businesses remain compliant while reducing the risk of penalties and reputational damage.

Risk Assessment: Leveraging advanced algorithms and AI-driven analytics, VigiTrust's risk assessment tools provide actionable insights into potential vulnerabilities. This proactive approach enables organizations to address risks before they escalate into major incidents.

Training and Awareness Programs: Recognizing the critical role of human behavior in cybersecurity, VigiTrust offers comprehensive training programs that empower employees with the knowledge and skills to identify and mitigate cyber threats.

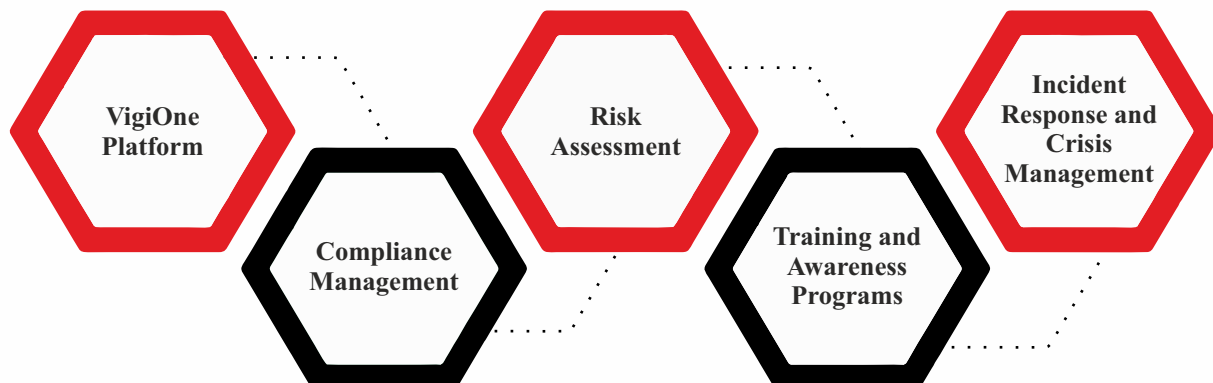
Incident Response and Crisis Management: In the event of a cyber incident, VigiTrust's experts provide rapid response services to contain the breach, mitigate damage, and restore operations. Their crisis management solutions ensure business continuity and minimize downtime.



VigiOne: Revolutionizing Compliance Management

At the heart of VigiTrust's offerings is **VigiOne**, an award-winning platform that simplifies compliance management. Designed to address the complexities of modern cybersecurity, VigiOne integrates project management capabilities, advanced training modules with over 200 courses, and collaboration tools to streamline communication between organizations and external assessors.

VigiOne's adaptability is one of its standout features. With built-in support for AI and automation, the platform anticipates emerging threats and adjusts to changes in regulatory requirements. The platform's user-friendly interface and advanced analytics make it a powerful tool for decision-makers. This ensures that organizations across industries—whether retail, banking, or healthcare—can rely on VigiOne to stay compliant and secure.



Overcoming Industry Challenges with Tailored Solutions

The industries VigiTrust serves face unique challenges, from protecting sensitive customer data to mitigating risks of payment fraud. For instance, retailers must comply with PCI DSS standards, while financial institutions grapple with stringent regulations such as GDPR and CCPA. VigiTrust's solutions are designed to address these challenges head-on, providing businesses with practical tools to safeguard their assets and maintain compliance.

The **Global Advisory Board** plays a crucial role in tackling these challenges. By bringing together a diverse range of perspectives, VigiTrust ensures that its solutions remain relevant and effective in addressing the ever-evolving cybersecurity landscape.

Staying Ahead of Emerging Trends

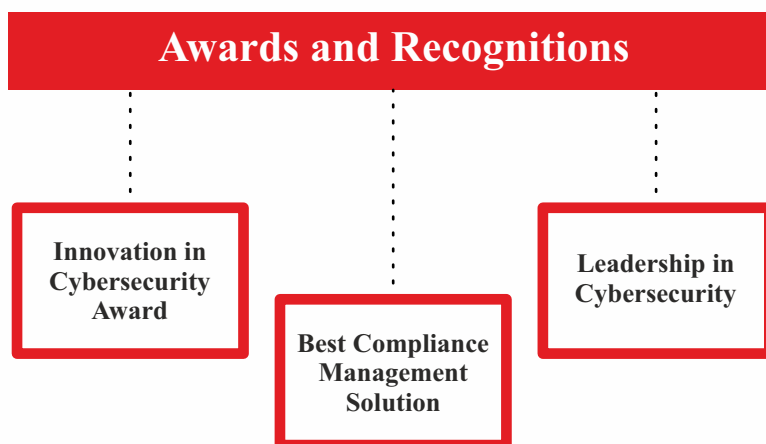
In a world where cyber threats are becoming increasingly sophisticated, staying ahead requires constant innovation. VigiTrust recognizes this and prioritizes proactive solutions to address new risks. By leveraging the 5 Pillars of Security Framework™, the company helps organizations adopt a holistic approach to cybersecurity, ensuring that no aspect of their operations is left vulnerable.

Additionally, VigiTrust's commitment to continuous learning and collaboration positions it as a thought leader in the industry. The company actively participates in regulatory discussions, ensuring that its solutions align with the latest standards and best practices.

A Culture of Collaboration and Empowerment

VigiTrust's success is built on a foundation of collaboration, both internally and externally. Mathieu has cultivated a company culture that values open communication, creativity, and employee empowerment. By encouraging team members to take ownership of projects and contribute their unique ideas, VigiTrust fosters an environment where innovation thrives.

VigiTrust's contributions to the cybersecurity industry have been widely recognized. The company has received numerous awards for its innovative solutions and thought leadership. Some of its notable accolades include:



Awards and Recognitions

- **Innovation in Cybersecurity Award:** Recognizing VigiTrust's commitment to developing groundbreaking solutions.
- **Best Compliance Management Solution:** Awarded for the effectiveness of the VigiOne platform in ensuring regulatory compliance.
- **Leadership in Cybersecurity:** Honoring Mathieu's contributions as a thought leader and advocate for cybersecurity awareness.

These awards underscore VigiTrust's position as a leader in the cybersecurity space and its unwavering commitment to excellence.



Shaping the Future of Cybersecurity

Looking ahead, VigiTrust is poised to continue its trajectory of growth and innovation. As businesses navigate an increasingly complex digital landscape, several trends are likely to shape the future of cybersecurity. The rise of AI-driven threats, the growing emphasis on data privacy, and the proliferation of IoT devices are just a few of the challenges organizations will face.

VigiTrust's response to these challenges is rooted in its commitment to adaptability and collaboration. By expanding initiatives like the Global Advisory Board and investing in cutting-edge technologies, the company aims to remain at the forefront of cybersecurity innovation. Mathieu's vision is clear: to make cybersecurity accessible, scalable, and impactful for businesses of all sizes.

Building a Resilient Cybersecurity Posture

For organizations looking to strengthen their cybersecurity strategies, Mathieu offers valuable insights. First and foremost, businesses must prioritize continuous learning. Staying informed about emerging threats and regulatory changes is essential for maintaining a robust security posture.

Collaboration is another key pillar. Engaging with industry experts, participating in forums, and fostering partnerships can provide organizations with the insights and resources they need to tackle complex challenges. Finally, accountability and transparency must be embedded in an organization's culture. By modeling these principles, leaders can create an environment where cybersecurity is viewed as a shared responsibility.

Conclusion

VigiTrust's journey is a testament to the transformative power of visionary leadership, collaboration, and innovation. Under Mathieu's guidance, the company has redefined how businesses approach Integrated Risk Management, providing practical solutions to complex cybersecurity challenges. As the digital landscape continues to evolve, VigiTrust remains committed to driving progress, fostering collaboration, and shaping the future of cybersecurity on a global scale.

Key Takeaways from the Transformative Journey of **VigiTrust**

1.

Innovative Cybersecurity Framework

VigiTrust's 5 Pillars of Security Framework™ offers a structured and holistic approach to managing risks across physical security, people, data, infrastructure, and crisis management.

2.

Visionary Leadership

CEO Mathieu has redefined cybersecurity with his human-centric, collaborative approach, leveraging over two decades of expertise in global compliance frameworks.

3.

VigiOne Platform

VigiOne simplifies compliance and risk management with AI-driven insights, real-time assessments, and adaptable tools, making it invaluable across industries.

4.

Global Collaboration

The VigiTrust Global Advisory Board unites industry leaders to address evolving cybersecurity challenges through innovation and shared expertise.

5.

Future-Focused Innovation

VigiTrust is shaping the future of cybersecurity by addressing AI-driven threats, IoT vulnerabilities, and regulatory changes with scalable, proactive solutions.







FOOD

Gloria Bonilla, 33 years old, lives in a 3x2ft² room, all her family have lived there, *her dream, to become the only one to move on.*



Best

CYBERSECURITY TOOLS

for Companies in the USA

The United States stands at the forefront of global FinTech innovation, with a dynamic ecosystem encompassing everything from challenger banks and digital payment solutions to algorithmic trading platforms and blockchain-based financial services. This rapid evolution, however, has also made US FinTech companies prime targets for increasingly sophisticated cyber threats. The sheer volume of sensitive financial and personal data handled by these firms, combined with the interconnectedness of modern financial systems, elevates cybersecurity from a mere IT concern to a fundamental business imperative.

US FinTechs face a complex threat landscape, including persistent and evolving risks such as ransomware attacks, phishing and social engineering, data breaches, insider threats, and vulnerabilities in APIs and third-party integrations. Moreover, the regulatory environment in the US is multifaceted and stringent. Key regulations and frameworks influencing FinTech cybersecurity include:

- 
- **Gramm-Leach-Bliley Act (GLBA):** Mandates financial institutions to explain their information-sharing practices to customers and safeguard sensitive data.
 - **Sarbanes-Oxley Act (SOX):** While primarily focused on financial reporting, SOX indirectly impacts cybersecurity by requiring robust internal controls, including those related to IT systems and data security for publicly traded companies.
 - **New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR Part 500):** A highly influential regulation that applies to any financial institution operating under NYDFS licensure, requiring comprehensive cybersecurity programs, risk assessments, and incident response plans.
 - **Securities and Exchange Commission (SEC) Cybersecurity Rules:** Mandates public companies to disclose material cybersecurity incidents within four business days and provides detailed disclosures on cybersecurity risk management and governance.
 - **NIST Cybersecurity Framework (CSF):** While voluntary, the NIST CSF provides a widely adopted set of guidelines and best practices for managing cybersecurity risk, particularly for critical infrastructure sectors, including financial services.
 - **Payment Card Industry Data Security Standard (PCI DSS):** A mandatory standard for organizations that process, store, or transmit credit card data.
 - **State-specific data privacy laws:** Such as the California Consumer Privacy Act (CCPA), which imposes strict requirements on the handling of consumer data.

To navigate this intricate web of threats and regulations, US FinTech companies must deploy a comprehensive arsenal of cybersecurity tools. This article outlines the best cybersecurity tools essential for building a resilient and secure FinTech operation in the United States.

Identity and Access Management (IAM)

Effective IAM is the cornerstone of FinTech security, controlling who can access what, when, and how. Given the diverse range of internal users, external partners, and customer interactions, robust IAM is non-negotiable.

- **Multi-Factor Authentication (MFA) and Adaptive Authentication:** Beyond simple passwords, MFA requires users to verify their identity through multiple methods (e.g., password + biometric, security token, or mobile app push notification). Adaptive authentication takes this further by dynamically adjusting the level of authentication based on risk factors like user location, device, and behavior. This is crucial for NYDFS compliance, which mandates strong authentication for accessing non-public information.
- **Role-Based Access Control (RBAC):** Implementing RBAC ensures that employees only have the minimum necessary access to systems and data required for their job functions (principle of least privilege). This significantly reduces the attack surface and potential damage from compromised accounts.
- **Privileged Access Management (PAM):** PAM solutions are designed to secure, manage, and monitor privileged accounts (e.g., administrator accounts) that have elevated access rights. These accounts are prime targets for attackers, and PAM helps prevent misuse and provides detailed audit trails.
- **User Behavior Analytics (UBA):** UBA tools leverage AI and machine learning to analyze user activity patterns and identify anomalous behavior that could indicate a compromised account or insider threat.

Key Tools



Data Loss Prevention (DLP) and Encryption

Protecting sensitive financial data, customer PII (Personally Identifiable Information), and proprietary information is paramount for US FinTechs, particularly due to GLBA and state-specific privacy laws.

- **Data Loss Prevention (DLP) Solutions:** DLP tools are designed to monitor, detect, and prevent sensitive data from leaving the organization's control. They can identify specific types of confidential information (e.g., Social Security numbers, credit card details) and block their unauthorized transmission via email, cloud storage, or removable media. Advanced DLP solutions utilize content inspection, contextual analysis, and machine learning for accurate detection.
- **Data Encryption:** All sensitive data, both at rest (stored on servers, databases, endpoints) and in transit (during transmission over networks, APIs), must be encrypted using strong, industry-standard algorithms (e.g., AES-256 for data at rest, TLS 1.3 for data in transit). Many compliance frameworks, including NYDFS, explicitly require encryption for non-public information.

Key Tools: Symantec DLP, Forcepoint DLP, McAfee DLP, Digital Guardian, Proofpoint.

API Security Solutions

FinTech companies heavily rely on Application Programming Interfaces (APIs) for interoperability, integrating with payment processors, data providers, and other financial services. Unsecured APIs are a significant vulnerability.

- **API Gateway and Firewall:** An API gateway acts as a central entry point for all API traffic, enforcing security policies, performing authentication and authorization, and rate limiting requests. An API firewall specifically protects APIs from various attacks, including those listed in the OWASP API Security Top 10.
- **API Security Testing (DAST, SAST, IAST):** Integrating security testing into the Secure Software Development Life Cycle (SSDLC) is crucial. Dynamic Application Security Testing (DAST) tests APIs in a running state, identifying runtime vulnerabilities. Static Application Security Testing (SAST) analyzes source code for flaws during development. Interactive Application Security Testing (IAST) combines elements of both.
- **Runtime API Protection:** These solutions provide real-time protection by monitoring API traffic for malicious activity and automatically blocking attacks. They often leverage AI and machine learning to detect anomalous behavior and respond proactively.

Key Tools: Akamai API Security, Salt Security, Nona Security, Cequence Security, Cloudflare API Shield.

Fraud Detection and Prevention Tools

Given the transactional nature of FinTech, robust fraud detection and prevention mechanisms are essential for protecting both the company and its customers from financial losses and reputational damage.

- **AI/ML-powered Fraud Detection:** Artificial Intelligence and Machine Learning algorithms can analyze vast datasets of transaction information, user behavior, and historical patterns in real-time to identify and flag suspicious activities indicative of fraud. These systems continuously learn and adapt to new fraud schemes.
- **Behavioral Biometrics:** These technologies analyze unique user behaviors (e.g., typing patterns, mouse movements, device usage) to verify identity and detect anomalies that might signal an account takeover attempt or synthetic identity fraud.
- **Transaction Monitoring Systems:** These systems continuously track and analyze financial transactions for signs of fraud, money laundering, or other illicit activities, often incorporating rules-based engines alongside AI/ML capabilities.
- **Know Your Customer (KYC) and Anti-Money Laundering (AML) Solutions:** While not solely cybersecurity tools, robust KYC and AML processes are foundational for fraud prevention and compliance with regulations like the Bank Secrecy Act (BSA). They involve verifying customer identities and monitoring transactions to prevent financial crime.

Key Tools: Feedzai, SEON, LexisNexis Risk Solutions, FICO Falcon Platform, Verafin.

Security Information and Event Management (SIEM) & Security Orchestration, Automation, and Response (SOAR)

Centralized visibility, threat intelligence, and rapid incident response are critical for US FinTechs navigating complex regulatory landscapes and sophisticated attacks.

- **SIEM:** SIEM solutions collect, aggregate, and analyze security logs and event data from various sources across the IT infrastructure (networks, servers, applications, security devices). They use correlation rules and advanced analytics to identify potential threats, generate alerts, and provide a holistic view of the security posture.
- **SOAR:** SOAR platforms automate and orchestrate incident response workflows. They integrate with various security tools, enabling automated actions such as blocking malicious IPs, isolating compromised endpoints, or enriching alerts with threat intelligence. SOAR helps reduce manual effort, improve response times, and ensure consistent incident handling, crucial for SEC and NYDFS incident reporting requirements.
- **User and Entity Behavior Analytics (UEBA):** Often integrated with SIEM, UEBA focuses on profiling the normal behavior of users and entities to detect subtle deviations that could indicate insider threats or targeted external attacks.

Key Tools: Splunk Enterprise Security, IBM QRadar, Microsoft Sentinel, Exabeam, Securonix, Palo Alto Networks Cortex XSOAR.

Vulnerability Management and Penetration Testing

Proactive identification and remediation of security weaknesses are essential for maintaining a strong security posture and adhering to frameworks like NIST CSF and NYDFS.

- **Vulnerability Assessment (VA) Tools:** VA tools scan systems, applications, and networks for known vulnerabilities, providing a prioritized list of weaknesses based on severity and exploitability.
- **Penetration Testing (Pentest) Services:** Penetration testing simulates real-world cyberattacks to identify exploitable vulnerabilities and assess the effectiveness of existing security controls. Regular, independent penetration testing for web applications, mobile applications, cloud infrastructure, and APIs is crucial for FinTechs. Many reputable firms specialize in these services for the US market.
- **Attack Surface Management (ASM):** ASM tools continuously discover and monitor an organization's digital assets (both known and unknown) to identify and manage external attack surfaces and potential entry points for attackers.
- **Secure Software Development Life Cycle (SSDLC) Tools:** Integrating security into every stage of software development, from design to deployment, helps build secure applications from the ground up. This includes using tools for secure code analysis (SAST, DAST, IAST) and software composition analysis (SCA) to identify vulnerabilities in open-source components.

Key Tools: Tenable Nessus, Qualys, Rapid7 InsightVM (for VA), HackerOne, Bugcrowd (for bug bounty programs and pentesting services), Synopsys, Checkmarx (for SSDLC).



tenable
Nessus Expert



RAPID7
insightVM



hackerone



bugcrowd



SYNOPSYS

Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP)

- Given the prevalent adoption of cloud services (AWS, Azure, GCP) by US FinTechs, dedicated cloud security tools are non-negotiable.
- **CSPM:** CSPM solutions continuously monitor cloud environments to identify misconfigurations, compliance violations (e.g., against CIS Benchmarks or custom policies), and security risks across various cloud services. They help ensure adherence to regulatory requirements and best practices.
- **CWPP:** CWPPs protect workloads (virtual machines, containers, serverless functions) running in the cloud. They provide threat detection, vulnerability management, and runtime protection for cloud-native applications, regardless of their underlying infrastructure.
- **Cloud Access Security Brokers (CASB):** CASBs act as a security policy enforcement point between cloud service users and cloud service providers, extending security controls to SaaS applications. They help enforce data security, compliance, and threat protection for cloud-based data.

Key Tools: Palo Alto Networks Prisma Cloud, CrowdStrike Falcon Cloud Security, Wiz, Orca Security, Zscaler (for CASB).

Endpoint Detection and Response (EDR) / Extended Detection and Response (XDR)

Endpoints (laptops, desktops, mobile devices) remain frequent entry points for cyberattacks. EDR and XDR solutions provide advanced threat detection and response capabilities for these devices and beyond.

- **EDR:** EDR tools monitor endpoint activity for suspicious behaviors that might indicate malware, ransomware, fileless attacks, or other advanced threats. They offer visibility into endpoint events and enable automated response actions like threat containment and device isolation.
- **XDR:** XDR takes EDR a step further by integrating security data from multiple sources across the IT stack (endpoints, networks, cloud, email, identity) to provide a more holistic view of threats and enable correlated detection and response. This is particularly valuable for complex, multi-stage attacks.

Key Tools: CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint, Trend Micro Apex One, Cortex XDR (Palo Alto Networks).

Web Application Firewall (WAF)

Web applications are often the primary interface for FinTech services and are frequently targeted by attackers. A robust WAF is essential.

- **WAF:** A WAF protects web applications from various attacks, including SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and other OWASP Top 10 vulnerabilities. It inspects HTTP traffic and filters out malicious requests before they reach the application.

Key Tools: Cloudflare WAF, Akamai Kona Site Defender, F5 Advanced WAF, Imperva, AWS WAF.

Cyber Insurance

While not a direct cybersecurity tool, cyber insurance is a crucial risk management strategy for FinTech companies in the US, providing a financial safety net in the event of a cyber incident.

- **Financial Coverage:** Cyber insurance policies can cover various costs associated with a cyberattack, including legal expenses, regulatory fines, data breach notification costs, forensic investigation fees, business interruption losses, and even ransomware payments.
- **Incident Response Support:** Many policies offer access to pre-approved incident response services, including cybersecurity legal counsel, forensic investigators, and public relations specialists, which can be invaluable during a crisis.

Key Providers in the US: Chubb, AIG, Travelers, Beazley, Coalition, At-Bay.



Building a Resilient FinTech Security Posture

Selecting the right cybersecurity tools is merely one component of a robust security strategy. US FinTech companies must also prioritize:



Adherence to Regulatory Frameworks

Continuously mapping their security controls and processes to relevant regulations (GLBA, NYDFS, SEC rules, PCI DSS, NIST CSF) and demonstrating compliance.



Security Awareness Training

Regularly educating all employees about cybersecurity best practices, phishing awareness, and recognizing social engineering tactics.



Robust Incident Response Plan

Developing and regularly testing a comprehensive plan for detecting, responding to, and recovering from cyber incidents, including clear communication protocols for regulatory bodies and affected parties.





Third-Party Risk Management

Thoroughly vetting and continuously monitoring the cybersecurity posture of all third-party vendors and partners that have access to sensitive data or systems. The Target breach, for instance, highlighted the critical importance of supply chain security.



Threat Intelligence Integration

Leveraging up-to-date threat intelligence to understand emerging threats, attack patterns, and vulnerabilities specific to the FinTech industry.



Security by Design

Integrating security principles into the very architecture and development of FinTech products and services from the outset.



The US FinTech landscape is characterized by its innovation and rapid evolution. However, this dynamism must be underpinned by an unwavering commitment to cybersecurity. By strategically implementing a layered defense using the best-in-class tools and fostering a strong security culture, FinTech companies in the USA can effectively mitigate risks, protect sensitive data, maintain customer trust, and ensure their continued growth and success in the digital economy.



A detailed oil painting of a gorilla in a lush, dense jungle. The gorilla is positioned on the left side of the frame, partially obscured by thick foliage. Its dark, shaggy fur is rendered with visible brushstrokes, and its white chest and face are highlighted. The gorilla appears to be looking towards the right. The background is a dense wall of green leaves and branches, with light filtering through in some places, creating a sense of depth and atmosphere. The overall style is realistic with a painterly texture.

Discover
new worlds
every week

Børneavisen

[The Children's Newspaper]



Top **5** **Antivirus
Software**
for Businesses in 2025
An In-Depth Review



Your business data is at risk if you're not using the right protection; nobody knows when a cyberattack will strike. Years of hard work, customer trust, and important files can go to waste in seconds. Hackers are not only targeting big companies anymore; small and mid-sized businesses are now their favorite targets because they often have weaker defenses, so they don't need to struggle too much.

No matter whether you're running an online business, small, mid-sized or large-scale, having reliable antivirus software is no longer a choice - it's a necessity.

In this article, you'll learn about the top 5 antivirus software for businesses in 2025, their features, pros and cons, and who they're best suited for so that you can easily choose which one is better for your business to keep it safe and secure.

1. Bitdefender GravityZone Business Security

Bitdefender is like a strong shield for your business. This antivirus software for businesses stops new and hidden threats before they cause any trouble. It also helps you keep your computers updated and protected, all from one simple dashboard. Perfect if you want strong protection without slowing things down.

Features

- Stops new and unknown threats
- Easy to manage many computers from one place
- Also helps update and fix software

Pros	Cons
• Excellent malware detection • Minimal system impact • Easy to scale and manage	• Advanced features may require IT expertise

Best for? Medium to large enterprises.

Price

Starts at \$77.69 per year for 3 devices. More devices can be added for an extra charge.

Customer Support:

Available 24/7 via live chat, email, and phone support. You also get access to an online knowledge base with helpful guides and FAQs.

2. CrowdStrike Falcon Pro

CrowdStrike is super quick at finding and blocking threats. As powerful antivirus software for businesses, it works through the cloud, stays always up-to-date, and doesn't take up much space on your devices. If you want fast, smart security without the heavy load, this is a great pick.

Features

- Catches threats quickly
- Lightweight, doesn't need much space
- Always updated in real-time

Pros	Cons
• Industry-leading threat visibility • Fast deployment • High accuracy in detecting advanced threats	• Premium pricing

Best for? Enterprises and high-security environments.

Price

Starts at \$99.99 per device per year. There's also a lighter plan at \$59.99 per device per year.

Customer Support:

Offers 24/7 phone support and online chat. Additionally, you get a knowledge base and detailed online resources to help troubleshoot any issues.



3. Norton Small Business Security

Norton gives your business real-time protection from viruses and backs up your important files in the cloud. This easy-to-use antivirus software for businesses protects computers, Macs, and phones all in one plan. It's a smart choice if you want simple, reliable security for a small team.

Features

- Real-time protection against viruses
- Cloud backup to save important files
- Protects computers, Macs, and smartphones

Pros

- Simple interface
- Covers PCs, Macs, and smartphones
- Affordable

Cons

- Lacks advanced EDR/XDR features

Best for? Small businesses and solo entrepreneurs.

Price

Starts at \$99.99 per year for 5 devices. You can upgrade to cover more devices for an additional cost.

Customer Support:

24/7 support via live chat, phone, and email. Norton also provides a detailed help center and FAQs for quick self-service

4. Sophos Intercept X

Sophos is smart — it learns from new threats and keeps getting better at protecting your business. As trusted antivirus software for businesses, it's really good at stopping ransomware attacks and lets you manage everything online easily. Perfect for businesses that need strong, smart, and growing protection.

Features

- Learns from threats to improve protection
- Stops ransomware before it locks your files
- Easy to manage online

Pros	Cons
• Strong behavioral analysis • Great for layered security strategies • Good for remote device management	• Slightly complex setup for non-technical users

Best for? SMBs and mid-size companies.

Price

Starts at \$28 per user per year for the basic plan, with advanced plans costing \$48 per user per year.

Customer Support:

Sophos offers 24/7 phone support, email, and a support portal for online help, as well as an extensive knowledge base for troubleshooting.

5. SentinelOne Singularity Control

SentinelOne works fast and can fix problems by itself, even undoing damage caused by ransomware. This advanced antivirus software for businesses gives you a clear view of all your devices without slowing them down. It's an excellent choice if you need powerful, automatic security for a tech-savvy team.

Features

- Automatically removes threats
- Can undo damage from ransomware
- Works very fast

Pros	Cons
• Fast, autonomous response • Advanced telemetry and visibility • Low system overhead	• Overkill for very small companies

Best for? Tech-savvy SMBs and larger enterprises.

Price

Starts at \$79.99 per device per year.

Customer Support:

Provides 24/7 support via phone, email, and chat. You also get access to a support portal and knowledge base for additional resources.

Feature Comparison

To help you make the more informed decision, here's a quick comparison of the key features of each antivirus software for businesses. Check out the detailed breakdown below to compare the features and find the antivirus software that best fits your business needs.

Feature	Bitdefender GravityZone	CrowdStrike Falcon	Norton Small Business	Sophos Intercept X	SentinelOne Singularity
Free Trial	Yes (30 days)	Yes (30 days)	Yes (7 days)	Yes (30 days)	No
Money-Back Policy	60 days	30 days	30 days	30 days	30 days
Endpoint Security	Yes	Yes	No	Yes	No
Centralized Management	Yes	Yes	Yes	Yes	Yes
Behavior-Based Detection	Yes	Yes	Yes	Yes	Yes
Operating Systems	Windows, macOS, iOS, Android	Windows, macOS, Linux, iOS, Android, ChromeOS	Windows, macOS, Android	Windows, macOS, Windows Server	Windows, macOS, Linux, iOS, Android, ChromeOS
Max Devices Supported	20	100	5	999	Unlimited

Conclusion

Protecting your business from hackers, viruses, and ransomware is not anymore a choice - it's crucial today for all-sized businesses. The above top 5 antivirus software for businesses offer strong protection to keep your data safe, improve system performance, and ensure everything runs smoothly. You can pick one of them looking at your preferences and needs.





IT'S TIME TO FOCUS
ON OUR WATERWAYS

Help us protect the
places you love to fish
Visit ozfish.org.au



The background of the entire image is a dark blue gradient. On the right side, there is a large, stylized shield shape. Inside the shield, there is a glowing blue hexagonal pattern, resembling a molecular or network structure. A large, white, 3D-style keyhole is positioned on the right side of the shield. At the bottom of the shield, there is a bright, starburst-like light source. Below the shield, there are faint, glowing lines and patterns that look like binary code or data streams.

Cyber

Pro

**SUBSCRIBE
to our Newsletter!**

Subscribe to our newsletter to
get our newest articles instantly!

www.cybrpro.com